

ABSTRACT OF THE DISCLOSURE

[0036] A method and a system by which to achieve authentication intrusion detection so as to effectively detect and prevent unauthorized access to and use of a local computer system, or the like, and take appropriate measures. The local system authentication process is redirected to an authenticator broker system (i.e. a secondary authentication system) that makes use of the local system authentication process paths and the local system authenticator file. The authenticator broker system includes an authenticator broker system file having stored therein secret authenticators of prospective users, a mapping file to assign a replacement identifier for the identifier entered by a particular user at the local system and redirected to the secondary system, and a decoy authenticator file to assign a decoy authenticator for the secret authenticator entered by the user and originally stored in the local system authentication file. It is the decoy authenticator that is captured and unknowingly used by the intruder to give away his or her presence. By way of example, the authenticator broker system may be a mainframe computer that is responsible for authentication and access control with respect to a local computer system.